

DMP:JAM/EHS
F. #2019R01707

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----- X

UNITED STATES OF AMERICA

- against -

NIKOLAY GOLTSEV,
SALIMDZHON NASRIDDINOV and
KRISTINA PUZYREVA

Defendants.

AFFIDAVIT AND
COMPLAINT IN SUPPORT
OF AN APPLICATION FOR
ARREST WARRANTS

(T. 18, U.S.C., §§ 554, 1349 and 2; T. 50,
U.S.C., §§ 4819(a)(1), 4819(a)(2)(A)-(G)
and 4819(b))

No. 23-M-956

----- X

EASTERN DISTRICT OF NEW YORK, SS:

Yevgeny Gershman, being duly sworn, deposes and states that he is a Special Agent with the United States Department of Homeland Security, Homeland Security Investigations, duly appointed according to law and acting as such:

Wire Fraud Conspiracy

In or about and between January 2022 and October 2023, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants NIKOLAY GOLTSEV, SALIMDZHON NASRIDDINOV and KRISTINA PUZYREVA, together with others, did knowingly and intentionally conspire to devise a scheme and artifice to defraud one or more U.S. companies by means of materially false and fraudulent pretenses, representations and promises, and for the purpose of executing such scheme and artifice, to transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce, writings, signs, signals, pictures and sounds, to wit:

electronic communications, emails and other online communications and monetary transfers in and through the Eastern District of New York and elsewhere, contrary to Title 18, United States Code, Section 1343.

(Title 18, United States Code, Section 1349)

Smuggling Goods from the United States

In or about and between January 2022 and October 2023, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants NIKOLAY GOLTSEV, SALIMDZHON NASRIDDINOV and KRISTINA PUZYREVA, together with others, did knowingly and fraudulently export and send from the United States, merchandise, articles and objects, to wit: items on the Commerce Control List set forth in Title 15, Code of Federal Regulations, part 774, Supplement Number 1, and items on the Common High Priority List set forth in Title 15, Code of Federal Regulations, part 746, supplement number 4, contrary to United States laws and regulations, to wit: Title 50, United States Code, Sections 4819(a)(1), 4819(a)(2)(A)-(G) and 4819(b) and Title 15, Code of Federal Regulations, Sections 736.2, 746.5(a)(1)(ii) and 746.8(a)(1), and did fraudulently and knowingly receive, conceal and facilitate the transportation and concealment of such merchandise, articles and objects, prior to exportation, knowing the same to be intended for exportation contrary to such United States laws and regulations.

(Title 18, United States Code, Sections 554(a) and 2)

Conspiracy to Violate the Export Control Reform Act ("ECRA")

In or about and between January 2022 and October 2023, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants NIKOLAY GOLTSEV, SALIMDZHON NASRIDDINOV and KRISTINA

PUZYREVA, together with others, did knowingly and willfully conspire to violate and to cause one or more violations of licenses, orders, regulations and prohibitions issued under the Export Control Reform Act, Title 50, United States Code, Sections 4810 et seq.

It was a part and an object of the conspiracy that the defendants NIKOLAY GOLTSEV, SALIMDZHON NASRIDDINOV and KRISTINA PUZYREVA, together with others, would and did agree to export and cause to be exported from the United States to Russia items on the Commerce Control List, as set forth in Title 15, Code of Federal Regulations, Part 774, Supplement Number 1, and items on the Common High Priority List, as set forth in Title 15, Code of Federal Regulations, Part 746, Supplement Number 4, without having first obtained a license for such export from the U.S. Department of Commerce.

(Title 50, United States Code, Sections 4819(a)(1), 4819(a)(2)(A)-(G) and 4819(b))

The source of your deponent's information and the grounds for his belief are as follows:¹

1. I am a Special Agent with the United States Department of Homeland Security, Homeland Security Investigations and have been since 2016. I am responsible for conducting and assisting in investigations into the activities of individuals and criminal groups responsible for unlawful proliferation of sensitive and military technologies, export

¹ Because the purpose of this complaint is to set forth only those facts necessary to establish probable cause to arrest, I have not described all the relevant facts and circumstances of which I am aware. Communications referenced herein that have been translated into English are in draft form.

control violations and espionage by foreign governments and related criminal and counterintelligence activity. Through my training, education and experience, I am familiar with the techniques and methods of operation used by individuals involved in intelligence and criminal activities to conceal their behavior from detection by law enforcement authorities. I have participated in numerous investigations, during the course of which I have conducted physical and electronic surveillance, interviewed witnesses, examined financial records, executed court-authorized search warrants and used other techniques to secure relevant information.

2. I am familiar with the facts and circumstances set forth below from my participation in the investigation, my review of documents obtained pursuant to the investigation and reports of other law enforcement officers involved in the investigation. When I rely on statements made by others, such statements are set forth only in part and in substance unless otherwise indicated.

I. The Export Control Reform Act and Export Administration Regulations

3. On August 13, 2018, the President signed into law the National Defense Authorization Act of 2019, which included the Export Control Reform Act (“ECRA”). See 50 U.S.C. § 4801 et seq. ECRA provided permanent statutory authority for the Export Administration Regulations (“EAR”), Title 15, Code of Federal Regulations, Parts 730-774.

4. ECRA provided that “the national security and foreign policy of the United States require that the export, reexport, and in-country transfer of items, and specified activities of United States persons, wherever located, be controlled.” 50 U.S.C. § 4811. To that end, ECRA granted the President the authority to “(1) control the export, reexport,

and in-country transfer of items subject to the jurisdiction of the United States, whether by United States persons or foreign persons; and (2) the activities of United States persons, wherever located, relating to” specific categories of items and information. 50 U.S.C. § 4812. ECRA granted to the Secretary of Commerce the authority to establish the applicable regulatory framework. 50 U.S.C. § 4813.

5. Through the EAR, the U.S. Department of Commerce’s Bureau of Industry and Security (“BIS”) reviewed and controlled the export from the United States to foreign destinations of certain items. In particular, BIS placed restrictions on the export and reexport of items that it determined could make a significant contribution to the military potential or nuclear proliferation of other nations or that could be detrimental to the foreign policy or national security of the United States. Under the EAR, such restrictions depended on several factors, including the technical characteristics of the item, the destination country, the end user and the end use of the item.

6. The most sensitive items subject to EAR controls were identified on the Commerce Control List (“CCL”) set forth in Title 15, Code of Federal Regulations, Part 774, Supplement Number 1. Items listed on the CCL were categorized by Export Control Classification Number (“ECCN”), each of which was subject to export control requirements depending on destination, end use and end user of the item.

7. Since February 24, 2022, when Russia launched its invasion of Ukraine, BIS has implemented a series of stringent export controls that restrict Russia’s access to the technologies and other items that it needs to sustain its attack on Ukraine. As of April 8, 2022, license requirements for exports, reexports and transfers to or within Russia

were expanded to cover all items on the CCL. See 87 Fed. Reg. 12226 (Mar. 3, 2022); 87 Fed. Reg. 22130 (Apr. 14, 2022); 15 C.F.R. § 746.8.

8. On March 3, 2022, BIS imposed additional license requirements for exports, reexports and transfers to or within Russia of any items subject to the EAR that were identified under certain Schedule B or Harmonized Tariff Schedule 6 (“HTS”) numbers. See 87 Fed. Reg. 12856 (March 8, 2022); 15 C.F.R. Part 746, Supp. No. 4. HTS codes took their first six digits from the corresponding Harmonized System (“HS”) code, which was a standardized numerical method of classifying traded products that was used by customs authorities around the world.

9. On September 14, 2023, working in conjunction with the United Kingdom and European Union, BIS published a “Common High Priority Items List,” which identified items by their corresponding HS codes that Russia sought to procure for its weapons programs. See <https://www.bis.doc.gov/index.php/all-articles/13-policy-guidance/country-guidance/2172-russia-export-controls-list-of-common-high-priority-items>. According to BIS, these priority items posed a heightened risk of being diverted illegally to Russia because of their importance to Russia’s war efforts.

10. Through the EAR, BIS also published the Entity List, which identified certain foreign persons—including businesses, research institutions, government and private organizations, individuals and other types of legal persons—that were subject to specific export license requirements and policies, in addition to those found elsewhere in the EAR, due to a determination that such persons had engaged in activities contrary to U.S. national security and/or foreign policy interests. See 15 C.F.R. § 744.11; 15 C.F.R. Part 744, Supp. No. 4 (the Entity List).

11. An exporter generally was required to file Electronic Export Information (“EEI”) through the Automated Export System (“AES”) where, among other reasons, an export license was required or the value of the commodity being exported was more than \$2,500. 15 C.F.R. § 758.1. The EEI required an exporter to list, among other things, the destination country, the ultimate consignee’s name and address, the intermediate consignee’s name and address, and a description of the commodity to be exported. Failure to file EEI or providing false or misleading information in EEI was a violation of ECRA (see, e.g., 50 U.S.C. 4819(a)(2)(F)), the EAR (see 15 C.F.R. Part 758), 13 U.S.C. § 305 and the Foreign Trade Regulations (see 15 C.F.R. Par 30).

12. Under ECRA, it was a crime to willfully violate, attempt to violate, conspire to violate or cause a violation of any regulation, order, license or authorization issued pursuant to the statute, including the EAR. See 50 U.S.C. § 4819(a)(1).

II. The Defendants and Relevant Entities

13. OOO² Radioavtomatika (“Radioavtomatika”) is a Russian defense procurement firm based in Moscow, Russia that specializes in procuring foreign items, including U.S.-origin items, for Russia’s defense industry. On or about March 3, 2022, following Russia’s invasion of Ukraine, BIS added Radioavtomatika to its Entity List, which identifies foreign parties that are subject to additional export restrictions and license requirements. See 87 Fed. Reg. 13141 (Mar. 9, 2022). Also on or about March 3, 2022,

² “OOO” is the abbreviation for the Russian business entity type, “общество с ограниченной ответственностью,” which means limited private company and is roughly the equivalent of a limited liability company or LLC in the United States.

pursuant to Executive Order 14024, the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") added Radioavtomatika to its Specially Designated Nationals and Blocked Persons ("SDN") List; U.S. persons are generally prohibited from dealing with individuals and entities on the SDN List.

14. OOO Testkomplekt ("Testkomplekt") is a Moscow-based electronic components distributor specializing in semiconductors and microelectronics that was established in or about 2016. Testkomplekt has held a variety of contracts with Russian military entities, including State Corporation Rostec, a Moscow-based defense conglomerate. On or about May 19, 2023, pursuant to Executive Order 14024, OFAC added Testkomplekt to its SDN List.

15. OOO NEVA-EKB ("EKB-Neva") is a Moscow-based supplier of electronic components, including radio components, microcircuits, connectors, resonators, diodes, capacitors and resistors. On or about May 19, 2023, pursuant to Executive Order 14024, OFAC added EKB-Neva to its SDN List.

16. The defendant NIKOLAY GOLTSEV is a dual Russian and Canadian national who resides in Canada. GOLTSEV served as an account manager and purchasing coordinator for Electronic Network, Inc. ("Electronic Network"), a company based in Montreal, Canada. On or about February 24, 2023, BIS added Electronic Network to its Entity List. See 88 Fed. Reg. 12170 (Feb. 27, 2022).

17. The defendant SALIMDZHON NASRIDDINOV is a dual national of Russia and Tajikistan who resides in Brooklyn, New York. NASRIDDINOV is a published author regarding integrated systems and other electronic technologies. On or about June 11, 2021, NASRIDDINOV founded SH Brothers Group Inc. ("SH Brothers"), a company with

listed addresses in Brooklyn, New York. On or about January 30, 2023, NASRIDDINOV founded SN Electronics, Inc. (“SN Electronics”), a company with listed addresses in Brooklyn, New York. SN Electronics was registered in NASRIDDINOV’s wife’s name.

18. The defendant KRISTINA PUZYREVA is a dual Russian and Canadian national who resides in Canada. PUZYREVA is married to GOLTSEV.

19. Co-conspirator 1 is a Russian national who resides in Russia. Co-conspirator 1 conducted procurement operations for multiple Russian entities through Suntronic F.Z.E. (“Suntronic”), a front company in the United Arab Emirates (“UAE”).

20. Co-conspirator 2 is a Russian national who resides in Russia and conducted procurement operations for Testkomplekt.

21. Co-conspirator 3 is a Russian national who resides in Russia and conducted procurement operations for EKB-Neva.

22. Co-conspirator 4 is a Russian national who resides in Russia and served as the procurement manager for Radioavtomatika. In or about August 2022, Co-conspirator 4 left Radioavtomatika and began working for another Moscow-based electronics distributor, OOO Komtech (“Komtech”).

III. Overview of the Criminal Scheme

23. As described below, records obtained from court-authorized search warrants and other evidence, including business records such as invoices, shipping documents, wire transfers and financial documents, as well as customs records from the U.S. and foreign countries, have revealed that GOLTSEV, NASRIDDINOV, PUZYREVA and others have been involved in smuggling U.S.-origin dual-use electronics to Russia. Using the SH Brothers and SN Electronics corporate entities, the defendants sourced, purchased

and exported to Russia millions of dollars of dual-use electronics from U.S. manufacturers and distributors located in the Eastern District of New York and elsewhere. Many of these items required a license from BIS to be exported to Russia. Even for items that did not require such a license, the defendants made and caused to be made false and misleading statements in EEI to conceal the fact that Russia was the ultimate end destination and that certain entities and individuals in Russia were the ultimate end users. As such, the defendants and their co-conspirators caused U.S. companies to sell and export electronic components in violation of ECRA and other U.S. laws and regulations; process and accept payments in furtherance of such illicit transactions; and file false documents and fail to file documents with BIS and other U.S. government agencies, including required statements regarding the ultimate consignee and purchaser. The defendants and their co-conspirators also caused U.S. financial institutions to process millions of dollars in payments in violation of U.S. laws and regulations. Many of these transactions were processed through bank accounts held by SH Brothers and SN Electronics and correspondent accounts at New York City banks in New York City and within the Eastern District of New York.

24. Specifically, Russian companies that sought to acquire particular parts or items from the United States were relayed to GOLTSEV. GOLTSEV communicated directly with U.S. manufacturers and distributors, typically using aliases such as “Nick Stevens” and “Gio Ross.” In those communications, GOLTSEV misrepresented and omitted material information, including information about how the items would be used, the various parties involved in the transactions, and the identities of the ultimate Russian end users.

25. GOLTSEV and NASRIDDINOV then purchased the items, including electronic components and integrated circuits, from U.S. companies. NASRIDDINOV received the items at various addresses he controlled in Brooklyn, New York, where he supervised their repackaging and export. GOLTSEV and NASRIDDINOV exported these items from the United States and transshipped them to Russia and Russian end users, including Radioavtomatika, Komtech, Testkomplekt and EKB-Neva, through a variety of intermediary companies in Turkey, Hong Kong, China, India, the UAE and elsewhere. Some of these intermediary companies received U.S. exports solely from SH Brothers, including Robotronix Semiconductors LTD (“Robotronix”), which was listed as an intermediate consignee on approximately 32 shipments valued at more than \$600,000, ostensibly for end users in China. BIS added Robotronix to its Entity List on October 6, 2023. See 88 Fed. Reg. 70352 (Oct. 11, 2023).

26. Some of the electronic components and integrated circuits sourced, purchased and exported by the defendants were designated as “Tier 1” items on the Common High Priority Items List, which, according to BIS, were of the highest concern due to their critical role in the production of advanced Russian precision-guided weapons systems, Russia’s lack of domestic production, and limited global manufacturers. Indeed, some of the same makes, models and part numbers of electronic components exported by the defendants through SH Brothers were found in seized Russian weapons platforms and signals intelligence equipment in Ukraine, including the Torn-MDM radio reconnaissance complex, the RB-301B “Borisoglebsk-2” electronic warfare complex, the Vitebsk L370 airborne counter missile system, Ka-52 helicopters, the Izdeliye 305E light multi-purpose guided missile, Orlan-10 unmanned aerial vehicles (“UAVs”) and T-72B3 battle tanks.

27. GOLTSEV and NASRIDDINOV were aware that the electronics being shipped had potential military applications. In a February 23, 2023 message, NASRIDDINOV wrote to GOLTSEV, “Happy Defender of the Fatherland,” referring to the holiday in Russia and parts of the former Soviet Union celebrating those who served in the armed forces. NASRIDDINOV attached to the message a screenshot showing activity in an SH Brothers bank account. GOLTSEV responded, “happy holiday to you too my friend, we are defending it in the way that we can [smile emoji].”

A. GOLTSEV’s Relationship with Military End Users in Russia

28. Returns from court-authorized search warrants, as well as other evidence, shows GOLTSEV’s long-standing relationships with Radioavtomatika, Testkomplekt, EKB-Neva and other Russia-based entities. GOLTSEV has procured electronic components for such entities for more than 12 years.

29. Communications involving GOLTSEV and Russian procurement agents, including Co-conspirator 4 and others, described efforts to evade U.S. export controls and other laws and the fact that the electronic components were destined for military users in Russia. For example, in a text message exchange between GOLTSEV and Co-conspirator 4 on or about December 22, 2016, GOLTSEV advised that he “fully understands that this [ordered electronic component] is military in nature,” which Co-conspirator 4 directed GOLTSEV to “definitely send to Radioavtomatika, like in our agreement.” In another message exchange between GOLTSEV and Co-conspirator 4 on or about January 17, 2017, GOLTSEV stated, “I understand that this is a military end user” and recommended that Radioavtomatika should test the parts in their laboratory. In a subsequent message, Co-conspirator 4 advised GOLTSEV that Co-conspirator 4 was waiting for “the military to sign

the contract” before placing the order. In or about October 2021, Co-conspirator 4 again advised GOLTSEV that paperwork regarding an order of electronics stated that the items were destined for Russia. In response, GOLTSEV told Co-conspirator 4, “in that case, bill to World Jetta”—a reference to World Jetta (H.K.) Logistics Ltd., a Hong Kong company that BIS added to its Entity List on or about June 28, 2022—but confirmed that he would nevertheless send it to Radioavtomatika in Russia. In a message exchange on or about October 31, 2022, Co-conspirator 4’s subordinate employee asked GOLTSEV, “please tell me do you have these goods, [they are] priceless in Russia,” and listed several different electronic components, including coaxial switches and capacitors, that were barred from being shipped to Russia. GOLTSEV responded with price quotes for the items.

30. Communications between GOLTSEV and Russian procurement agents, including Co-conspirator 2, reflected a sophisticated understanding of U.S. export controls and sanctions. For example, on or about December 30, 2022, in a message exchange with Co-conspirator 2 regarding an order placed through SH Brothers, GOLTSEV requested “separate invoices . . . the ECCN[s] aren’t very pretty. We’ll ship them piecemeal.” In a message on or about February 23, 2023, GOLTSEV told Co-conspirator 2 that “Elnet [Electronic Network] got sanctioned . . . do me a favor. If anyone ever asks about me, don’t tell them who I am, where I am, etc. . . . Elnet’s been in trouble for a long time because they exported a lot to Russia.” Nevertheless, GOLTSEV confirmed he would be able to complete sales for “microchips, transistors, [and] circuits” because “we work with China, not Russia, therefore all is good.” In a subsequent conversation, Co-conspirator 2 again queried GOLTSEV about “any other USA companies that don’t mind selling to China.” GOLTSEV responded, “we have one for emergencies, but we’re keeping them as a last

resort.” Based on my training and experience, I assess that the reference to “China” was intended as a cover for the fact that GOLTSEV was using China as a transshipment location sending these controlled items to Russia.

31. GOLTSEV also received requests from Co-conspirator 3 to obtain items on the CCL that were controlled for anti-terrorism reasons. For example, on or about December 16, 2022, in response to a query, GOLTSEV advised Co-conspirator 3 that “76 pcs, you can buy them here with ECCN 3A991c.3.” In message on or about February 1, 2023, Co-conspirator 3 asked GOLTSEV, “ECCN: 5A991.b.4 can you get this?” and included a screenshot of a product from a Texas-based electronics distributor (“Texas Company 1”). Similarly, in a message on or about February 6, 2023, Co-conspirator 3 asked GOLTSEV, “can you get this ECCN? 4A994I.” Later, in a message on or about February 22, 2023, Co-conspirator 3 requested “40 pcs ECCN 5A991.b.1. Can you get this?” Between November 2022 and February 2023, SH Brothers made nine shipments to Co-conspirator 3 in Russia through a Turkish intermediary company.

B. The Establishment and Use of SH Brothers

32. Following the imposition of additional sanctions and export controls in response to Russia’s invasion of Ukraine in February 2022, GOLTSEV, NASRIDDINOV and PUZYREVA began using SH Brothers to facilitate illicit exports to Russia.

33. In a text message exchange between NASRIDDINOV and GOLTSEV on or about and between June 8, 2022 and June 9, 2022, NASRIDDINOV stated, “I spoke with the guys, we will set it up through America, I got to Moscow, tomorrow will also have a meeting, we decided upon logistics, if you have people in Moscow we can also meet and discuss the scheme so that they would pick up from Moscow.” GOLTSEV responded that

he had “many orders,” but that it was “becoming difficult to do business here [in Canada through Electronic Network], maybe it will be easier to do through the US . . . everything is loaded from the USA . . . everything that needs to be received, payment place the orders, get the goods together and unload it in any ‘friendly’ country.”

34. In or about and between August 2022 and September 2023, U.S. Customs and other records show that SH Brothers exported more than 250 shipments of electronic components, valued at more than \$7 million, to third-country transshipment companies; the shipments were then unlawfully diverted to Russia. During this same period, financial records, including wire transactions through correspondent accounts at New York City banks and within the Eastern District of New York, reflected millions of dollars in payments from Russian entities to these transshipment companies.

35. For example, in or about and between March 2023 and May 2023, SH Brothers shipped approximately \$404,949 worth of integrated circuits and other electronics to Co-conspirator 1 and his front company Suntronic in the UAE, which were then sent to Petersburg Intelligent Transport Logistics, a Russian entity that OFAC added to its SDN list on or about May 19, 2023. Notably, the Internet Protocol (“IP”) address for Suntronic, which was used to communicate with GOLTSEV about the orders, corresponded to a location in St. Petersburg, Russia, rather than the UAE.

C. SH Brothers Shipments to Testkomplekt, Komtech and Suntronic

36. In or about and between September 2022 and November 2022, customs and other records show that SH Brothers exported approximately 15 shipments of electronic components, valued at approximately \$352,000, to Testkomplekt in Russia through a Hong Kong intermediary company (“Hong Kong Company 1”). These exports included a

shipment on or about September 8, 2022 of connectors manufactured by a Texas company; a shipment on or about September 15, 2022 of connectors manufactured by a Pennsylvania and Switzerland-based company; a shipment on or about September 28, 2022 of computer modules manufactured by a Minnesota company; and a shipment on or about October 2, 2022 of converters manufactured by a Massachusetts company.

37. In or about November 2022, U.S. Customs and Border Protection (“CBP”) detained several shipments made by SH Brothers to Hong Kong Company 1 that were ultimately destined for Testkomplekt in Russia. In electronic message exchanges, Co-conspirator 2 repeatedly queried GOLTSEV about the status of these detained shipments and provided GOLTSEV with false information that GOLTSEV could use to respond to CBP inquiries. GOLTSEV communicated with CBP using the alias “Nick Stevens” and an SH Brothers email address with the signature “Procurement Department” and the SH Brothers’s Brooklyn, New York address. When asked about Hong Kong Company 1’s principal, GOLTSEV responded that the person had a Chinese-sounding surname rather than a Russian one.

38. In or about August 2022, SH Brothers made a shipment of microchips to Co-conspirator 4’s company, Komtech, through a Turkish intermediary (“Turkish Company 1”). These microchips had a Tier 1 HTS code listed on the Common High Priority Items List and required a license from BIS to be exported to Russia. Co-conspirator 4 acted as a go-between with GOLTSEV and Komtech’s founder and director. Specifically, in a message on or about August 31, 2022, Komtech’s founder and director requested that Co-conspirator 4 procure 3,000 microchips made by an Arizona-based manufacturer. Co-conspirator 4 sourced the microchips through GOLTSEV and SH

Brothers. SH Brothers received several payments from Turkish Company 1, including an October 3, 2022 payment for \$5,300. The wire details for this payment listed the part number of the microchips and denoted “QTY 2000.”

39. In a message exchange on or about April 21, 2023, Co-conspirator 4 and GOLTSEV discussed shipping the microchips through China or Turkey, ultimately deciding to make the shipment through Turkish Company 1 to “avoid problems.” GOLTSEV provided Co-conspirator 4 with an SH Brothers invoice for 3,000 pieces of the requested microchip. The invoice listed the applicable HTS codes and payment information for an SH Brothers bank account in Brooklyn, New York. Shipping records reflected that a package containing the microchips was mailed to SH Brothers from Texas Company 1 on or about April 17, 2023. Two days later, on or about April 25, 2023, the same items were sent by NASRIDDINOV to Turkish Company 1 in Turkey.

40. Between in or about November 2022 and August 2023, SH Brothers exported approximately 27 shipments, valued at approximately \$1,086,058, to Suntronic. These shipments were then sent to Russian end users including Petersburg Intelligent Transportation Logistics. One such shipment on or about June 23, 2023 was for transceivers carrying a Tier 1 HTS code listed on the Common High Priority Items List, which required a license from BIS to be exported to Russia. These types of transceivers have been found in Russian UAVs in Ukraine. Notably, Suntronic received approximately \$15 million from Petersburg Intelligent Transportation Logistics in or about and between October 2022 and February 2023.

41. GOLTSEV communicated with Co-conspirator 1 to facilitate these shipments. In a message exchange on or about January 9, 2023, GOLTSEV informed Co-

conspirator 1 that he needed an “end user declaration,” to which Co-conspirator 1 responded, “darn.” GOLTSEV replied, “or at least let me know what end user to put in there and then send it tomorrow, but it needs to match the application.” Co-conspirator 1 responded, “then lets put the one we used last time,” and the two agreed to falsely list a UAE company as the end user.

42. Similarly, in or about February and March 2023, GOLTSEV and Co-conspirator 1 also communicated about falsifying the names of end users. In a message in or about February 2023, GOLTSEV advised Co-conspirator 1 to “write something more substantial [to the U.S. company] so that there are no more questions.” Co-conspirator 1 responded, “is it better to provide them with a Chinese end user,” to which GOLTSEV stated, “yes should be ok.” In a message on or about March 3, 2023, Co-conspirator 1 asked GOLTSEV if it was possible to make one shipment paid “via the Chinese company,” since “each one separately so expensive, or does it mean extra trouble at customs?” GOLTSEV responded, “no sir, more than 50-60 will trigger a lot of interest it’s better to break it up.”

D. The Establishment of SN Electronics

43. On or about and between November 8, 2022 and November 15, 2022, GOLTSEV and NASRIDDINOV exchanged a series of messages in which GOLTSEV commented that shipping to Russia via third countries had become “dangerous” and discussed a shipment of electronic components that had been detained by U.S. officials at John F. Kennedy International Airport (“JFK Airport”) in Queens, New York. NASRIDDINOV responded that “Ukrainians alleged that they’re being bombed from parts from there [a U.S. company], maybe that’s why they started investigating everything?”

GOLTSEV replied, “we need to figure out why they keep holding the package . . . I don’t really understand how they figured [it] out.” In a subsequent message, on or about November 9, 2022, GOLTSEV commented that, “in the future we will need to load from several companies, not to attract attention . . . for now large packages will be dangerous until we understand what they figured out . . . we will need to think of diversifying the load . . . so that not everything is moving from the same deck.”

44. In response to increased scrutiny from U.S. officials, including the delay or detention of several outbound shipments from SH Brothers at JFK Airport, in or about January 2023, GOLTSEV and NASRIDDINOV began using SN Electronics to order and export electronic components. In a text message exchange on or about and between January 31, 2023 and February 10, 2023, NASRIDDINOV confirmed to GOLTSEV that the “new company is already functioning . . . Its called SN Electronics.” GOLTSEV responded, “Wonderful sir. Eagerly waiting for Tax ID sir. We had problems with some large orders from [Texas Company 1] . . . we will reorder later from SN.” NASRIDDINOV later provided GOLTSEV with SN Electronics’ registered address in Brooklyn, New York, which was also the address of a restaurant that NASRIDDINOV controlled.

45. GOLTSEV and NASRIDDINOV then used SN Electronics to obtain approximately \$36,871 worth of non-reflective switches from Texas Company 1 for Co-conspirator 2 and Testkomplekt. These non-reflective switches had Tier 1 HTS codes that were included on the Common High Priority Items List and required a license from BIS to be exported to Russia.

46. GOLTSEV and NASRIDDINOV initially placed the order for these non-reflective switches from Texas Company 1 through SH Brothers. In or about January

2023, Texas Company 1 cancelled the order for SH Brothers and told GOLTSEV that the “manufacturer requires that shipments of this product be direct to an END CUSTOMER from an AUTHORIZED DISTRIBUTOR only.” Subsequently, GOLTSEV placed the same order through SN Electronics, using the alias “Gio Ross” in his email communications with Texas Company 1 and falsely claiming in an email on or about February 15, 2023 that SN Electronics was a “prototype and design manufacturing company.” Texas Company 1 shipped the order to an SN Electronics address in Brooklyn, New York on or about February 21, 2023. Once the shipment was made from Texas Company 1 to the SN Electronics address in Brooklyn—which, in reality, was NASRIDDINOV’s restaurant—shipping records revealed that, on or about February 27, 2023, the items were exported by NASRIDDINOV to Robotronix in Hong Kong, a transshipment company frequently utilized by Testkomplekt.

E. The Defendants Profited from the Criminal Scheme

47. The defendants and their co-conspirators profited from their criminal scheme. On or about September 15, 2022, in a text message from NASRIDDINOV to GOLTSEV, NASRIDDINOV boasted, “SH [Brothers] is one of the best companies in the world, it’s time to move forward onto the stock exchange and stock market, capital should be in the billions, we are working.” GOLTSEV responded, “pushing components to those who need it I can do, everything else you will have to teach me [three smile emojis].”

48. In a text message exchange on or about January 13, 2023, GOLTSEV complained to PUZYREVA that a subordinate of Co-conspirator 2 “asked me to make 80 accounts . . . I am making accounts for 3 mln [i.e., million]. Fingers hurting already from the laptop.” PUZYREVA responded, “Lot of money? We will get rich.” Later, on or about January 20, 2023, GOLTSEV messaged PUZYREVA, “Dasha [Co-conspirator 2’s

employee] paid. 700k.” Notably, financial records revealed wire transfers totaling approximately \$700,000 into an SH Brothers account on or about and between January 18, 2023 and January 26, 2023 from the Hong Kong-based Robotronix in connection with an order for Testkomplekt.

49. PUZYREVA utilized numerous bank accounts to make financial transactions in furtherance of the scheme. For example, PUZYREVA was the signatory on two New York-based bank accounts, one that listed NASRIDDINOV’s home address in Brooklyn, New York as the address of record. Statements for these accounts reflected large cash deposits made in Brooklyn that corresponded with trips that PUZYREVA and the GOLTSEV made from Canada to meet with NASRIDDINOV. Some of these deposits were in amounts just under \$10,000. Notably the Internal Revenue Service (“IRS”) maintains a transaction reporting requirement providing that any person who, during trade or business, receives more than \$10,000 cash in a single transaction is required report the transaction to the IRS. For example, on or about December 27, 2022, a \$9,800 cash deposit was made into one of PUZYREVA’s accounts at an automated teller machine (“ATM”) in Manhattan, New York. On or about May 23, 2022, a cash deposit of \$8,700 was made into one of PUZYREVA’s accounts at an ATM in Manhattan, while a \$4,000 deposit was made on the same day into the same account from an ATM in Brooklyn located near an address used by NASRIDDINOV and SH Brothers. On or about March 13, 2023, a cash deposit of \$9,700 was made into one of PUZYREVA’s accounts at an ATM in Manhattan. These deposits were then transferred to accounts held and used by PUZYREVA and GOLTSEV in Canada.

WHEREFORE, your deponent respectfully requests that an arrest warrant be issued for the defendants NIKOLAY GOLTSEV, SALIMDZHON NASRIDINOV and KRISTINA PUZYREVA, so that they may be dealt with according to law.

IT IS FURTHER REQUESTED that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including this Affidavit and any arrest warrants issued, with the exception that the complaint and arrest warrant can be unsealed for the limited purpose of disclosing the existence of, or disseminating, the complaint and/or arrest warrant to relevant United States, foreign or intergovernmental authorities, at the discretion of the United States and in connection with efforts to prosecute the defendant or to secure the defendant's arrest, extradition or expulsion. Based on my training and experience, I have learned that criminals actively search for criminal affidavits on the Internet and disseminate them to other criminals as they deem appropriate, such as by posting them publicly through online forums. Premature disclosure of the contents of this Affidavit and related documents will seriously jeopardize the investigation, including by giving targets an opportunity to flee or continue flight from

prosecution, destroy or tamper with evidence, change patterns of behavior and notify confederates.



Yevgeny Gershman
Special Agent
United States Department of Homeland Security,
Homeland Security Investigations

Sworn to before me this
30th day of October, 2023



THE HONORABLE LOIS BLOOM
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK